Security proof of practical quantum key distribution schemes

Yodai Watanabe
National Institute of Informatics, Research Organization of Information and Systems
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 1018430, Japan

(Dated: February 1, 2008)

This paper provides a security proof of the Bennett-Brassard (BB84) quantum key distribution protocol in practical implementation. To prove the security, it is not assumed that defects in the devices are absorbed into an adversary's attack. In fact, the only assumption in the proof is that the source is characterized. The proof is performed by lower-bounding adversary's Rényi entropy about the key before privacy amplification. The bound reveals the leading factors reducing the key generation rate.

PACS numbers: 03.67.Dd, 89.70.+c, 02.50.-r

One of the fundamental problems in cryptography is to provide a way of sharing a secret random number between two parties, Alice and Bob, in the presence of an adversary Eve. The quantum key distribution is a solution to this problem[1, 2]; indeed it allows Alice and Bob to generate a shared secret key securely against Eve with unbounded resources of computation. The security of quantum key distribution against general attacks was first proved by Mayers[10]. Later, Shor-Preskill[11] provided a simple security proof based on the observation that quantum key distribution (BB84 protocol) is closely related to quantum error-correcting codes (CSS codes). Gottesmann et al.[6] showed that the Shor-Preskill proof is still valid as long as the source and detector are perfect enough so that all defects can be absorbed into Eve's attack (see also [7, 12] for the rate achievability of quantum codes in the security proof). In contrast to the security proof based on quantum codes, the Mayers proof has a remarkable characteristics. Namely in the Mayers proof, although the source has to be (almost) perfect, there is no restriction on the detector; in particular, it can be uncharacterized. By exchanging the role of the source and detector in the Mayers proof, Koashi-Preskill[9] provided a security proof which applies to the case where the detector is perfect, but the source can be uncharacterized (except that the averaged states are independent of Alice's basis). The aim of this work is to generalize these results. We provide a security proof of the BB84 protocol in which the only assumption is that the source is characterized. In the same way as Koashi-Preskill[9], this can be transformed into a security proof which is based on characteristics of the detector. Further we note that the security proof also applies to the B92 protocol[1].

Let us first recall the BB84 protocol[2]. Let $\mathcal{H}$ be a Hilbert space. Let $\mathcal{A} = \{1, \cdots, N\}$, and for $\mathcal{B} \subset \mathcal{A}$ denote the cardinality of $\mathcal{B}$ by $n_{\mathcal{B}}$. The BB84 protocol is described as follows.

BB84 protocol: (i) Alice generates two binary strings $a^{\mathcal{A}} = \{a_i\}_{i\in\mathcal{A}}$ and $x^{\mathcal{A}} = \{x_i\}_{i\in\mathcal{A}}$ according to the probability distribution $p(a^{\mathcal{A}}, x^{\mathcal{A}}) = \prod_i p_{a_i,x_i}$. (ii) Bob generates a binary string $b^{\mathcal{A}} = \{b_i\}_{i\in\mathcal{A}}$ according to the probability distribution $p(b^{\mathcal{A}}) = \prod_i p_{b_i}$. (iii) Alice sends the quantum state on $\mathcal{H}^{\otimes N}$, $\rho^{\mathcal{A}}_{a,x} = \bigotimes_{i\in\mathcal{A}} \rho_{a_i,x_i}$, to Bob. (iv) Bob applies the measurement on $\mathcal{H}^{\otimes N}$, $\{E^{\mathcal{A}}_{b,y}\}_{y^{\mathcal{A}}} = \big\{ \bigotimes_{i\in\mathcal{A}} E_{b_i,y_i} \big\}_{y^{\mathcal{A}}\in\{0,1,\phi\}^N}$, to the received quantum state, where $E_{0,\phi} = E_{1,\phi}$ is the measurement corresponding to the result that Bob cannot detect a state. (v) Alice and Bob open $a^{\mathcal{A}}$ and $b^{\mathcal{A}}$ respectively. Let $\mathcal{D} = \{i \in \mathcal{A} | y_i \neq \phi\}$ and $\mathcal{C} = \{i \in \mathcal{D} | a_i = b_i\}$. Alice and Bob select a random subset $\mathcal{T} \subset \mathcal{C}$ (which does not necessarily satisfy $n_{\mathcal{T}}/n_{\mathcal{C}} \sim 1/2$). Let $\mathcal{K} = \mathcal{C} - \mathcal{T}$. (vi) Alice and Bob compare $x^{\mathcal{T}}$ and $y^{\mathcal{T}}$, and count the number of errors, $n^e_{\mathcal{T}} = |\{i \in \mathcal{T} | x_i \neq y_i\}|$. (vii) Bob estimates $x^{\mathcal{K}}$ by exchanging error-correction information with Alice. (viii) Alice and Bob generate a secret key s by applying a compression function to $x^{\mathcal{K}}$.

To prove the security of the BB84 protocol, the previous works[6, 9, 10, 11] assume that either Alice's source or Bob's detector is almost perfect in the sense that all defects in the device can be absorbed into Eve's attack. We wish to prove the security of quantum key distribution under practical implementation. Note that the previous security proofs have been based on directly bounding Eve's mutual information about the final key, i.e. the key after privacy amplification. In this work, we first lower-bound Eve's Rényi entropy about the key before privacy amplification, and then apply privacy amplification in the classical information theory which makes use of a compression function in a universal hash family (see [3] for the classical theory of privacy amplification).

We now provide basic definitions which will be used later (see e.g. [8] for details). The variation distance between probability distributions p and q is given by $d_V(p, q) = \frac{1}{2}\sum_\omega |p(\omega) - q(\omega)|$. The quantum analogue of the variation distance is called the trace distance. For an Hermitian operator X with the spectrum decomposition $X = \sum_i x_i E_i$, define the projection $\{X > 0\}$ by $\{X > 0\} = \sum_{i:x_i>0} E_i$. Then the trace distance between quantum states ρ and σ, $d_T(\rho, \sigma)$, is given by $d_T(\rho, \sigma) = \frac{1}{2}\mathrm{Tr}\,|\Delta| = \frac{1}{2}\mathrm{Tr}\,(\Delta\{\Delta > 0\} - \Delta\{-\Delta > 0\})$ with $\Delta = \rho - \sigma$. The trace distance can be bounded by another distance called the fidelity as $d_T(\rho, \sigma) \le \sqrt{1 - F(\rho, \sigma)^2}$, where the fidelity $F(\rho, \sigma)$ between ρ and σ is given by $F(\rho, \sigma) = \mathrm{Tr}\,|\sqrt{\rho}\sqrt{\sigma}|$.

Let z be the output of the measurement by Eve. Then, without loss of generality, the probability distribution of

the random variables can be written as

$$\begin{aligned} p_a^{\mathcal{C}}(x,y,z) &\equiv p(x^{\mathcal{C}},y^{\mathcal{C}},z|a^{\mathcal{A}},b^{\mathcal{A}},x^{\mathcal{T}},y^{\mathcal{T}},\mathcal{D},\mathcal{T}) \\ &= p_a^{\mathcal{C}}(x)\mathrm{Tr}\,(E_{a,y}^{\mathcal{C}}\otimes E_z)U(\rho_{a,x}^{\mathcal{C}}\otimes\rho_E)U^\dagger. \end{aligned}$$

Here, ρ_E is the initial state of an ancilla system $\mathcal{H}_E$ introduced by Eve, E_z is the Eve's measurement on the ancilla system, and U is the Eve's unitary operation acting on the composite system. (The quantum channel is assumed to be under Eve's control). For $\mathcal{B}\subset\mathcal{C}$ and p_a as above, let $p_a^{\mathcal{B}}$ denote the marginal distribution of the random variables defined on $\mathcal{B}$.

We begin with decomposing ρ_α $(a,x\in\{0,1\})$ as

$$\rho_{a,x}=p_{a,x}^{(0)}\rho_{a,x}^{(0)}+p_{a,x}^{(1)}\rho_{a,x}^{(1)},\quad \rho_{a,x}^{(0)},\rho_{a,x}^{(1)}\in\mathcal{S}(\mathcal{H}),\tag{1}$$

where $p_{a,x}^{(0)}+p_{a,x}^{(1)}=1$, $p_{a,x}p_{a,x}^{(0)}=p^{(0)}$ for a positive constant $p^{(0)}\le\min_{a,x}\{p_{a,x}\}$, and $\rho_{a,x}^{(0)}$ has a Schatten decomposition of the form

$$\rho_{a,x}^{(0)}=\sum_{k_{a,x}}\lambda_{a,x}(k_{a,x})|k_{a,x}\rangle\langle k_{a,x}|.\tag{2}$$

We note that $\rho_{a,x}$ always has a decomposition of the above form (where we allow $\rho_{a,x}^{(0)}=\rho_{a,x}^{(1)}$). Let $\mathcal{X}=\{(0,0),(0,1),(1,0),(1,1)\}$. We now construct a set of pure states, $\{\hat{\rho}_\alpha\}_{\alpha\in\mathcal{X}}$, such that there exists a physical transformation from $\{\hat{\rho}_\alpha\}_{\alpha\in\mathcal{X}}$ to $\{\rho_\alpha^{(0)}\}_{\alpha\in\mathcal{X}}$. Let $\mu_{\alpha\beta}$ $(\alpha,\beta\in\mathcal{X})$ be a mapping from $\{|k_\alpha\rangle\}_{k_\alpha}$ to $\{|k_\beta\rangle\}_{k_\beta}$ with $\mu_{\alpha\alpha}$ being the identity on $\{|k_\alpha\rangle\}_{k_\alpha}$, and introduce the Gram matrix G by writing

$$[G]_{\alpha\beta}=\sum_{k_\alpha}\sqrt{\lambda_\alpha(k_\alpha)\lambda_\beta(k_{\alpha\beta})}\langle k_\alpha|k_{\alpha\beta}\rangle\langle\phi_{k_\alpha}|\phi_{k_{\alpha\beta}}\rangle,$$

where $|k_{\alpha\beta}\rangle=\mu_{\alpha\beta}(|k_\alpha\rangle)$ and $|\phi_{k_\alpha}\rangle$ is a state on an ancilla system $\mathcal{H}_\phi$. Since $G\ge 0$, there exists a square matrix C such that $G=C^\dagger C$. Further, since all the diagonal elements of G are 1, we can define a pure state $\hat{\rho}_\alpha$ $(\alpha\in\mathcal{X})$ on a 4-dimensional Hilbert space $\mathcal{H}_4$ by

$$\hat{\rho}_\alpha=|C_\alpha\rangle\langle C_\alpha|,$$

where C_α denotes the α-th column of C. It follows from this construction that there exists a physical transformation from $\{\hat{\rho}_\alpha\}_{\alpha\in\mathcal{X}}$ to $\{\rho_\alpha^{(0)}\}_{\alpha\in\mathcal{X}}$ (see [4]). Now we introduce an approximation of $\{\hat{\rho}_\alpha\}_{\alpha\in\mathcal{X}}$ which is easier to treat in the security proof. Let $\mathcal{H}_2$ be a 2-dimensional subspace of $\mathcal{H}_4$, and $\sigma_{a,x}$ $(a,x\in\{0,1\})$ be states on $\mathcal{H}_2$ such that

$$\sigma_{0,0}+\sigma_{0,1}=\sigma_{1,0}+\sigma_{1,1}=I_{\mathcal{H}_2},$$

where, for a Hilbert space $\mathcal{H}$, $I_{\mathcal{H}}$ denotes the identity on $\mathcal{H}$. Note that the decompositions (1) and (2) and the choises of $\mu_{\alpha\beta}$, $|\phi_{k_\alpha}\rangle$ and $\sigma_{a,x}$ are not unique; they should be determined so that the distance $d_T(\sigma_{a,x},\hat{\rho}_{a,x})$ will be minimized. In the case of coherent states with no phase reference, $\rho_\alpha=\sum_{k\in\mathbb{N}}(\mu^k/k!)e^{-\mu}|k;\alpha\rangle\langle k;\alpha|$, for instance, we can take for $\alpha,\beta\in\mathcal{X}$ and $k\in\mathbb{N}$, $\rho_\alpha^{(0)}=\hat{\rho}_\alpha=\sigma_\alpha=|1;\alpha\rangle\langle 1;\alpha|$, $p_\alpha^{(0)}=\mu e^{-\mu}$, $\mu_{\alpha\beta}(|k;\alpha\rangle)=|k;\beta\rangle$ and $|\phi_{k;\alpha}\rangle=|\phi\rangle$.

The decomposition (1) allows us to consider that the Alice's source generates $\rho_{a,x}^{(0)}$ with probability $p_{a,x}^{(0)}$ and $\rho_{a,x}^{(1)}$ with probability $p_{a,x}^{(1)}$. Further, we assume that Eve is informed of partial information about each state ρ_A generated by the Alice's source: (i) $\rho_A=\rho_{a,x}^{(0)}$ or $\rho_A=\rho_{a,x}^{(1)}$ and (ii) $\rho_A=\rho_{0,x}^{(1)}$ or $\rho_A=\rho_{1,x}^{(1)}$ when $\rho_A=\rho_{a,x}^{(1)}$. This assumption is advantageous to Eve, and hence does not reduce the security of the protocol. Let $\mathcal{L}\subset\mathcal{K}$ be the positions where $\rho_{a,x}^{(0)}$ is generated, and $\mathcal{M}=\mathcal{K}-\mathcal{L}$. We now fix $\mathcal{L}$ and $\mathcal{M}$, and consider the best success probability to estimate $x^{\mathcal{M}}$ from $\rho_{a,x}^{(1)\mathcal{M}}$ and $a^{\mathcal{M}}$. Here note that we can estimate each bit x_i of $x^{\mathcal{M}}$ separately because each state ρ_{a_i,x_i} is generated independently of the other bits $\{x_{i'}|i'\ne i,i'\in\mathcal{M}\}$. For $a\in\{0,1\}$, let $\{T_{a,0},T_{a,1},T_{a,\phi}\}$ be a POVM on $\mathcal{H}$ which is used to discriminate $\rho_{a,0}^{(1)}$ and $\rho_{a,1}^{(1)}$, and let $p_a^{(1)}$ be the conditional probability defined by $p_a^{(1)}=(p_{a,0}p_{a,0}^{(1)}+p_{a,1}p_{a,1}^{(1)})/(p_{a,0}+p_{a,1})$. Further, define for a constant $\delta_{\mathcal{M}}^a>0$,

$$\begin{aligned} p_-^a &= (p_{\mathcal{M}}^a-\delta_{\mathcal{M}}^a)\frac{n_{\mathcal{D}}^a}{n_{\mathcal{K}}^a p_a^{(1)}},\quad p_{\mathcal{M}}^a=\frac{n_{\mathcal{M}}^a}{n_{\mathcal{A}}^a},\\ \epsilon_{\mathcal{M}}^a &= \exp(-n_{\mathcal{A}}^a D(B_1(p_{\mathcal{M}}^a)||B_1(p_{\mathcal{M}}^a-\delta_{\mathcal{M}}^a))), \end{aligned}$$

where $n_{\mathcal{B}}^d=|\{i\in\mathcal{B}|a_i=d\}|$ for $\mathcal{B}\subset\mathcal{A}$, B_1 denotes the Bernoulli distribution, and $D(p||q)$ is the relative entropy of p and q[13]. Here let us consider the condition C given by

$$C:\sum_{x,x'}\mathrm{Tr}\hat{p}_{a,x}^{(1)}\rho_{a,x}^{(1)}T_{a,x'}\ge p_-^a,$$

where $\hat{p}_{a,x}^{(d)}=p_{a,x}p_{a,x}^{(d)}/(p_{a,0}p_{a,0}^{(d)}+p_{a,1}p_{a,1}^{(d)})$ for $d\in\{0,1\}$. Then it can be verified that $\mathrm{Pr}_{\mathcal{A}}[\neg C]\le\epsilon_{\mathcal{M}}^a$, where the probability $\mathrm{Pr}_{\mathcal{A}}$ is taken over the randomness in choosing $\mathcal{D},\mathcal{T},\mathcal{L}\subset\mathcal{A}$ (see e.g. [5]). Suppose now that the condition C holds. Then we have

$$n_{\mathcal{M}}^a\le n_{\mathcal{M}}^{a+}\equiv\max_{\mathcal{M}}\{n_{\mathcal{M}}^a|p_-^a\le 1\}.$$

Also, we can write the best success probability of the discrimination as

$$s_{\mathcal{M}}^a=\sup_{T_{a,0},T_{a,1}:C}\left\{\frac{\sum_x\mathrm{Tr}\,\hat{p}_{a,x}^{(1)}\rho_{a,x}^{(1)}T_{a,x}}{\sum_{x,x'}\mathrm{Tr}\,\hat{p}_{a,x}^{(1)}\rho_{a,x}^{(1)}T_{a,x'}}\right\}.$$

Let z^* be a random variable induced by a measurement on $\rho_{a,x}^{\mathcal{K}}$. Then, by definition of $s_{\mathcal{M}}^a$, it follows that

$$p_a^{\mathcal{K}}(x|z^*)\le p_a^{\mathcal{L}}(x|z^*)(s_{\mathcal{M}}^0)^{n_{\mathcal{M}}^0}(s_{\mathcal{M}}^1)^{n_{\mathcal{M}}^1}.\tag{3}$$

Having considered the $\mathcal{M}$ part, we next consider the $\mathcal{L}$ part. Let us first estimate the error rate $p_{\mathcal{L}}^e$ at $\mathcal{L}$ from

$p^e_{\mathcal{T}} = n^e_{\mathcal{T}}/n_{\mathcal{T}}$, the error rate at $\mathcal{T}$. On remembering that the error probability of the discrimination at $\mathcal{M}$ is at least $1 - s^a_{\mathcal{M}}$ for a basis a, define for a constant $\delta_p > 0$,

$$p^+_{\mathcal{L}} = \frac{n_{\mathcal{K}} p^e_{\mathcal{T}} + n_{\mathcal{C}}\delta_p - n^0_{\mathcal{M}}(1 - s^0_{\mathcal{M}}) - n^1_{\mathcal{M}}(1 - s^1_{\mathcal{M}})}{n_{\mathcal{L}}},$$
$$\epsilon^e_{\mathcal{T}} = \exp\big(- n_{\mathcal{T}} D(B_1(p^e_{\mathcal{T}})||B_1(p^e_{\mathcal{T}} + \delta_p)\big).$$

Then we have $\Pr_{\mathcal{A}}[p^e_{\mathcal{L}} > p^+_{\mathcal{L}}] \le \mu_{\mathcal{L}} \equiv \epsilon^{\mathcal{M}}_0 + \epsilon^{\mathcal{M}}_1 + \epsilon^e_{\mathcal{T}}$, from which, it follows that

$$\sum_{x,y,z:|x\oplus y|>n_{\mathcal{L}}p^+_{\mathcal{L}}} p^{\mathcal{L}}_a(x, y, z) \le \mu_{\mathcal{L}}. \tag{4}$$

Now, let us consider a modified protocol in which Alice sends $\hat{\rho}^{\mathcal{L}}_{\bar{a},x}$ (instead of $\hat{\rho}^{\mathcal{L}}_{a,x}$), where $\bar{a}$ denotes the bit-wise inversion of binary string a. Let $p_{\bar{a}}$ be the corresponding conditional probability in the modified protocol. It then follows from the monotonicity of the trace distance that

$$d_V(p^{\mathcal{T}}_a(x, \tilde{y}, z), p^{\mathcal{T}}_{\bar{a}}(x, \tilde{y}, z)) \le d_T(\bar{\rho}^{\mathcal{L}}_a, \bar{\rho}^{\mathcal{L}}_{\bar{a}}), \tag{5}$$

where $\bar{\rho}_a = \frac{1}{2}\sum_x \hat{\rho}_{a,x}$ for $a \in \{0, 1\}$. We note that $d_T(\bar{\rho}^{\mathcal{L}}_a, \bar{\rho}^{\mathcal{L}}_{\bar{a}})$ can be bounded as $d_T(\bar{\rho}^{\mathcal{L}}_a, \bar{\rho}^{\mathcal{L}}_{\bar{a}}) \le \sqrt{1 - F(\bar{\rho}_0, \bar{\rho}_1)^{2n_{\mathcal{L}}}}$. From inequalities (4) and (5), it follows that

$$\sum_{x,y,z:|x\oplus y|>n_{\mathcal{L}}p^+_{\mathcal{L}}} p^{\mathcal{L}}_{\bar{a}}(x, y, z) \le \mu_{\mathcal{L}} + d_T(\bar{\rho}^{\mathcal{L}}_a, \bar{\rho}^{\mathcal{L}}_{\bar{a}}). \tag{6}$$

Let us now introduce the POVM $\{M_{a,yz}\}_{y,z}$ by writing

$$p^{\mathcal{L}}_a(x, y, z) = \mathrm{Tr}\,\hat{p}^{\mathcal{L}}_a(x)\hat{\rho}^{\mathcal{L}}_{a,x}M_{a,yz}$$

with $\hat{p}^{\mathcal{L}}_a(x) = \prod_{i\in\mathcal{L}} \hat{p}^{(0)}_{a_i,x_i} = 2^{-n_{\mathcal{L}}}$, where, for simplicity, we have omitted deviding the right-hand side by $\sum_{y,z} \mathrm{Tr}\,\bar{\rho}^{\mathcal{L}}_a M_{a,yz}$ because it will be canceled when we will consider the conditional probability $\hat{p}^{\mathcal{L}}_a(x|\tilde{y}, z)$. Now, let us consider the case where Bob uses the opposite basis $\bar{a}$ at $\mathcal{L}$ and introduce the notation $\tilde{y}$ by writing

$$p^{\mathcal{L}}_a(x, \tilde{y}, z) = \mathrm{Tr}\,\hat{p}^{\mathcal{L}}_a(x)\hat{\rho}^{\mathcal{L}}_{a,x}M_{\bar{a},yz}.$$

Note that $E_{0,0} + E_{0,1} = E_{1,0} + E_{1,1}$, and so $p^{\mathcal{L}}_a(x, z) = \sum_y p^{\mathcal{L}}_a(x, y, z) = \sum_y p^{\mathcal{L}}_a(x, \tilde{y}, z)$. That is, the probability distribution $p^{\mathcal{L}}_a(x, z)$ is independent of the basis used for the Bob's measurement. Thus, in the sequel, we will consider $p_a(x, \tilde{y}, z)$ rather than $p_a(x, y, z)$.

To examine the security of the protocol, it is more convenient to treat $\sigma_{a,x}$ than $\hat{\rho}_{a,x}$. Thus, define

$$\hat{p}^{\mathcal{L}}_a(x, \tilde{y}, z) = \mathrm{Tr}\,\hat{p}^{\mathcal{L}}_a(x)\sigma^{\mathcal{L}}_{a,x}M_{\bar{a},yz}.$$

The monotonicity of the trace distance gives

$$\begin{aligned} &d_V(p^{\mathcal{L}}_a(x, \tilde{y}, z), \hat{p}^{\mathcal{L}}_a(x, \tilde{y}, z)) \le \nu_{\mathcal{L}}, \\ &\nu_{\mathcal{L}} \equiv \sum_x \hat{p}^{\mathcal{L}}_a(x) d_T(\hat{\rho}^{\mathcal{L}}_{a,x}, \sigma^{\mathcal{L}}_{a,x}). \end{aligned} \tag{7}$$

This, together with (6), yields

$$\sum_{y,z} \mathrm{Tr}\,(\bar{\sigma}^{\mathcal{L}}_{\bar{a}} - \bar{\sigma}_{\tilde{y}})M_{\bar{a},yz} \le \mu_{\mathcal{L}} + \nu_{\mathcal{L}} + d_T(\bar{\rho}^{\mathcal{L}}_a, \bar{\rho}^{\mathcal{L}}_{\bar{a}}), \tag{8}$$

where we have defined

$$\bar{\sigma}_{\tilde{y}} = \sum_{x^{\mathcal{L}}:|x\oplus y|\le n_{\mathcal{L}}p^+_{\mathcal{L}}} \hat{p}^{\mathcal{L}}_a(x)\sigma^{\mathcal{L}}_{\bar{a},x}.$$

Inequality (8) can be seen as a restriction on Eve's measurement. To take advantage of this restriction, we now construct a projection on $\mathcal{H}^{\otimes n_{\mathcal{L}}}$, $P_{\tilde{y}}$, which sufficiently preserves $\bar{\sigma}_{\tilde{y}}$. For this purpose, let us first consider the problem of quantum hypothesis testing, where two hypotheses are, for fixed base $a \in \{0, 1\}$, $H_0 : \rho = \sigma_{a,0} \in \mathcal{H}_2$ and $H_1 : \rho = \sigma_{a,1} \in \mathcal{H}_2$. If $\{P_{a,x}\}_{x\in\{0,1\}}$, defined by

$$P_{a,x} = \{\sigma_{a,x} - \sigma_{a,\bar{x}} > 0\},$$

is used as a test for the hypothesis testing, then the success probability $s^a_{\mathcal{L}}$ is given by

$$s^a_{\mathcal{L}} = \frac{1}{2}(1 + d_T(\sigma_{a,0}, \sigma_{a,1})).$$

Suppose now that we receive a product state $\sigma^{\mathcal{L}}_{a,x}$ from the Alice's source, and estimate $x^{\mathcal{L}}$ by applying the above hypothesis testing to each individual state. Let k be an integer such that $0 \le k \le n_{\mathcal{L}}$. If we allow up to k errors in the estimation of $n_{\mathcal{L}}$-bit string $x^{\mathcal{L}}$, then the error probability ϵ^P (i.e. the probability that we make more than k errors) can be bounded as

$$\epsilon^P \le \left(2^{n_{\mathcal{L}}} - \frac{2^{n_{\mathcal{L}}h(\frac{k}{n_{\mathcal{L}}})}}{2\sqrt{n_{\mathcal{L}}}}\right)(s^0_{\mathcal{L}})^{\bar{n}^0_{\mathcal{L}}}(s^1_{\mathcal{L}})^{\bar{n}^1_{\mathcal{L}}}\left(\frac{1 - s^m_{\mathcal{L}}}{s^m_{\mathcal{L}}}\right)^k,$$

where $s^m_{\mathcal{L}} = \min\{s^0_{\mathcal{L}}, s^1_{\mathcal{L}}\}$, $\bar{n}^a_{\mathcal{L}} = n_{\mathcal{L}} - n^a_{\mathcal{L}}$, and we have used, for $0 \le k \le n$ and $0 \le q \le 1$,

$$\frac{2^{nh(\frac{k}{n})}}{2\sqrt{n}} \le \sum_{i=0}^{k} \binom{n}{i} q^i(1 - q)^{n-i} \le 2^{nh(\frac{k}{n})},$$

with $h(p) = -p \log p - (1 - p) \log(1 - p)$ (see e.g. [5]). We are now in position to construct $P_{\tilde{y}}$. Let $\delta_P = \frac{k}{n_{\mathcal{L}}}$ and $p^* = p^+_{\mathcal{L}} + \delta_P$. Define the projection $P_{\tilde{y}}$ on $\mathcal{H}^{\mathcal{L}}$ by

$$P_{\tilde{y}} = \sum_{x^{\mathcal{L}}:|x\oplus y|\le n_{\mathcal{L}}p^*} \bigotimes_{i\in\mathcal{L}} P_{\bar{a}_i,x_i}.$$

Then it can be verified that $\mathrm{Tr}\,\bar{\sigma}_{\tilde{y}}(I_{\mathcal{H}^{\mathcal{L}}} - P_{\tilde{y}}) \le \epsilon^P \mathrm{Tr}\,\bar{\sigma}_{\tilde{y}}$, which shows that $P_{\tilde{y}}$ is a required projection (provided that $1 - s^m_{\mathcal{L}}$ is sufficiently small).

Having constructed the projection $P_{a,x}$, we now bound the conditional probability $\hat{p}^{\mathcal{L}}_a(x|\tilde{y}, z)$. Since

$$\hat{p}^{\mathcal{L}}_a(\tilde{y}, z) = \mathrm{Tr}\,\bar{\sigma}^{\mathcal{L}}_a M_{\tilde{y}z} = \bar{\pi}_{\mathcal{L}} \equiv 2^{-n_{\mathcal{L}}}\mathrm{Tr}\,M_{\tilde{y}z}$$

with $M_{\tilde{y}z} = M_{\bar{a},yz}$ for short, we now bound $\hat{p}_a^{\mathcal{L}}(x, \tilde{y}, z)$. It follows, on using $\mathrm{Tr}\, P_{\tilde{y}} \leq 2^{n_{\mathcal{L}} h(p^*)}$, that

$$\mathrm{Tr}\, P_{\tilde{y}} p_a^{\mathcal{L}}(x) \rho_{a,x}^{\mathcal{L}} P_{\tilde{y}} M_{\tilde{y}z} \leq \pi_{\mathcal{L}},$$
$$\pi_{\mathcal{L}} \equiv 2^{-n_{\mathcal{L}} + n_{\mathcal{L}} h(p^*) + \bar{n}_{\mathcal{L}}^0 \log q_0 + \bar{n}_{\mathcal{L}}^1 \log q_1} \mathrm{Tr}\, M_{\tilde{y}z},$$

where, for $a \in \{0,1\}$, $q_a = \max_{x,x' \in \{0,1\}} \{\mathrm{Tr}\, \sigma_{a,x} P_{\bar{a},x'}\}$. Define now

$$\hat{p}'_a(x, \tilde{y}, z) = \mathrm{Tr}\, (I_{\mathcal{H}^{\mathcal{L}}} - P_{\tilde{y}}) \hat{p}_a^{\mathcal{L}}(x) \sigma_{a,x}^{\mathcal{L}} (I_{\mathcal{H}^{\mathcal{L}}} - P_{\tilde{y}}) M_{\tilde{y}z}.$$

Since $\bar{\sigma}_a^{\mathcal{L}} = \bar{\sigma}_{\bar{a}}^{\mathcal{L}} = (\bar{\sigma}_{\bar{a}}^{\mathcal{L}} - \bar{\sigma}_{\tilde{y}}) + \bar{\sigma}_{\tilde{y}}$, $P_{\tilde{y}}$ and $\bar{\sigma}_{\tilde{y}}$ commute, and $\sum_y \mathrm{Tr}\, \bar{\sigma}_{\tilde{y}} \leq 2^{n_{\mathcal{L}} h(p_{\mathcal{L}}^+)}$, we have

$$\sum_{x,y,z} \hat{p}'_a(x, \tilde{y}, z) = \sum_{x,y,z} \hat{p}_a^{\mathcal{L}}(x, \tilde{y}, z) \frac{\hat{p}'_a(x, \tilde{y}, z)}{\hat{p}_a^{\mathcal{L}}(x, \tilde{y}, z)} \leq \omega_{\mathcal{L}},$$
$$\omega_{\mathcal{L}} \equiv \mu_{\mathcal{L}} + \nu_{\mathcal{L}} + d_T(\bar{\rho}_a^{\mathcal{L}}, \bar{\rho}_{\bar{a}}^{\mathcal{L}}) + 2^{n_{\mathcal{L}} h(p_{\mathcal{L}}^+)} \epsilon^P.$$

Hence Markov's inequality for a constant $c > 0$ yields

$$\mathrm{Pr}_{\hat{p}_a} [\hat{p}'_a(x, \tilde{y}, z) \leq c \omega_{\mathcal{L}} \hat{p}_a^{\mathcal{L}}(x, \tilde{y}, z)] \geq 1 - c^{-1},$$

where c should be determined so that Eve's mutual information about the final key will be minimized. Further, Schwarz's inequality gives

$$\mathrm{Tr}\, P_{\tilde{y}} \hat{p}_a^{\mathcal{L}}(x) \sigma_{a,x}^{\mathcal{L}} (I_{\mathcal{H}^{\mathcal{L}}} - P_{\tilde{y}}) M_{a,yz} \leq (\pi_{\mathcal{L}} \hat{p}'_a(x, \tilde{y}, z))^{\frac{1}{2}}.$$

Therefore it follows that

$$\hat{p}_a^{\mathcal{L}}(x, \tilde{y}, z) \leq \left((\pi_{\mathcal{L}})^{\frac{1}{2}} + (\hat{p}'_a(x, \tilde{y}, z))^{\frac{1}{2}} \right)^2,$$

and so

$$\mathrm{Pr}_{\hat{p}_a} [\hat{p}_a^{\mathcal{L}}(x|\tilde{y}, z) > \Pi_{\mathcal{L}}] \leq \frac{1}{c}, \quad \Pi_{\mathcal{L}} \equiv \frac{\pi_{\mathcal{L}}}{\bar{\pi}_{\mathcal{L}} \left(1 - (c\omega_{\mathcal{L}})^{\frac{1}{2}}\right)^2}. \tag{9}$$

Now, it follows from inequality (3) that the conditional Rényi entropy $R_a^{\mathcal{K}}(X|\tilde{y}^{\mathcal{L}}, z)$ can be bounded as

$$R_a^{\mathcal{K}}(X|\tilde{y}^{\mathcal{L}}, z) \equiv -\log \sum_{x^{\mathcal{K}}} \left(p_a^{\mathcal{K}}(X = x|\tilde{Y} = \tilde{y}^{\mathcal{L}}, Z = z) \right)^2$$
$$\geq R_a^{\mathcal{L}}(X|\tilde{y}, z) + R_{a-}^{\mathcal{M}},$$

where $R_{a-}^{\mathcal{M}} = -\sum_a n_{\mathcal{M}}^a \log s_{\mathcal{M}}^a$, and a capital letter (say X) denotes the random variable which samples the corresponding small letter (say x). Now, using constraints (7) and (9), let us derive another constraint of the form

$$\mathrm{Pr}_{p_a} [R_a^{\mathcal{L}}(X|\tilde{y}, z) > R_{a-}^{\mathcal{L}}] \leq \epsilon_{\mathcal{L}}.$$

If $\nu_{\mathcal{L}} = 0$, for example, we can take $R_{a-}^{\mathcal{L}} = -\log \Pi_{\mathcal{L}}$ and $\epsilon_{\mathcal{L}} = c^{-1}$. Define

$$R_E^{\mathcal{K}} = \min_{\mathcal{M}: n_{\mathcal{M}}^a \leq n_{\mathcal{M}}^{a+}} \{R_{a-}^{\mathcal{L}} + R_{a-}^{\mathcal{M}}\},$$

and let m be an integer such that $l \equiv R_E^{\mathcal{K}} - m > 0$. Choose a function g at random from a universal family of hash functions from $\{0,1\}^n$ to $\{0,1\}^m$. If Alice and Bob choose $s = g(x^{\mathcal{K}})$ as their secret key, then the Eve's expected information about S, given Z and G, satisfies $I(S : Z, G) \leq n_{\mathcal{L}} \epsilon_{\mathcal{L}} + 2^{-l}/\ln 2$, where we consider $\tilde{Y}$ as an auxiliary random variable (see [3] for details). Here we note that $R_E^{\mathcal{K}}$ is not explicitly dependent on the characteristics of the detector, and hence the detector can be uncharacterized. Further, as $n_{\mathcal{L}} \to \infty$, the terms $\nu_{\mathcal{L}}$ and $d_T(\bar{\rho}_a^{\mathcal{L}}, \bar{\rho}_{\bar{a}}^{\mathcal{L}})$ approach to 1 unless $\hat{\rho}_{a,x} = \sigma_{a,x}$ and $\bar{\rho}_a^{\mathcal{L}} = \bar{\rho}_{\bar{a}}^{\mathcal{L}}$; this shows that the leading factors reducing the key generation rate are the asymmetries of the source represented by these terms.

To see that our result is consistent with the previous ones, suppose that the source and detector are perfect. In this case, we can take $\rho_{a,x}^{(0)} = \sigma_{a,x} = \rho_{a,x}$, $\mathcal{L} = \mathcal{K}$, $\mu_{\mathcal{L}} = \epsilon_T^e$, $\nu_{\mathcal{L}} = 0$, $d_T(\bar{\rho}_a^{\mathcal{L}}, \bar{\rho}_{\bar{a}}^{\mathcal{L}}) = 0$, $\log q_a = -1$, $\delta_P = 0$, $\epsilon^P = 0$. Since $\omega_{\mathcal{L}} = \epsilon_T^e \to 0$ as $n_{\mathcal{K}} \to \infty$ for fixed δ_p, $R_E^{\mathcal{K}}/n_{\mathcal{K}}$ approaches to $h(p_T^e)$ for sufficiently small c^{-1} and δ_p. This is consistent with the results in the previous works[6, 9, 10, 11][14].

We close this paper with mentioning some extensions of this work. (i) In the same way as Koashi-Preskill[9], we can provide a security proof of the BB84 protocol where the only assumption is that the detector and basis dependence of the averaged states are characterized. (ii) It is also of importance to give a security proof of the B92 protocol[1]. Suppose that the source generates ρ_0 with probability p_0 and ρ_1 with probability p_1. Then we decompose ρ_a $(a \in \{0,1\})$ as $\rho_a = p_0^{(0)} \rho_a^{(0)} + p_1^{(1)} \rho_a^{(1)}$ so that $p_0 p_0^{(0)} = p_1 p_1^{(1)}$. Again we define $\hat{\rho}_a$ by introducing the Gram matrix as above. Note that $\hat{\rho}_a$ is a pure state on a 2-dimensional Hilbert space $\mathcal{H}_2$. Hence, the terms $\nu_{\mathcal{L}}$ and $d_T(\bar{\rho}_a^{\mathcal{L}}, \bar{\rho}_{\bar{a}}^{\mathcal{L}})$ automatically vanish in this case, which could be considered as an advantage of the B92 protocol. More detailed investigation concerning these extensions will be the subject of future work.

The author is grateful to Dr. Keiji Matsumoto for comments. This work was supported in part by MEXT, Grant-in-Aid for Encouragement of Young Scientists (B) No. 15760289.

[1] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992)
[2] C. H. Bennett and G. Brassard, in *Proceedings of IEEE Conference on Computers, Systems and Signal Processing*, Banglore (India), 175–179 (1984)
[3] C. H. Bennett et al., IEEE Trans. Inform. Theory **41**, 1915 (1995)

[4] A. Chefles, R. Jozsa and A. Winter, quant-ph/0307227.

[5] I. Csizár and J. Körner, Information theory, coding theorems for discrete memoryless systems, Academic (1981)

[6] D. Gottesman et al., *Quantum Information and Computation* **4**, 325–360 (2004)

[7] M. Hamada, J. Phys. A: Math. and Gen. **37**, 8303 (2003)

[8] M. Hayashi, An Introduction to Quantum Information, Springer, to be published

[9] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003)

[10] D. Mayers, J. Assoc. Comput. Mach. **48**, 351 (2001)

[11] P. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000)

[12] S. Watanabe, R. Matsumoto and T. Uyematsu, quant-ph/0412070

[13] In the case where Eve is allowed to collapse Bob, $n^a_{\mathcal{M}}$ should be replaced by $n^a_{\mathcal{C}}$.

[14] The original bound given by Mayers[10] is slightly weaker (but this can be improved by a minor modification).